On second case of Strong Fermat's Last Theorem conjecture

Roland Quême

2013 Mai 28

Contents

Abstract

This article deals with a conjecture, introduced in [GQ] (hereinafter $SFLT2$), which generalizes the second case of Fermat's Last Theorem: *Let $p > 3$ be a prime. The diophantine equation $\frac{u^p+v^p}{u+v} = w_1^p$ with $u, v, u+v, w_1 \in \mathbb{Z}\backslash\{0\}$, u, v coprime and $v \equiv 0 \mod p$ has no solution.* Let ζ be a pth primitive root of unity and $K := \mathbb{Q}(\zeta)$. A prime q is said *p-principal* if the class of any prime ideal $\mathfrak{q}_K$ of K over q is a p-power of a class.

Assume that $SFLT2$ fails for (p, u, v). Let q be any odd prime coprime with puv, f the order of $q \mod p$, n the order of $\frac{v}{u} \mod q$, ξ a primitive nth root of unity, $\mathfrak{q}$ the prime ideal $(q, u\xi - v)$ of $\mathbb{Q}(\xi)$. In this complement of the article [GQ] revisiting some works of Vandiver, we prove that, if q is *p-principal* and $n \neq 2p$ then

$$\Big(\frac{1+\xi\zeta^k}{1+\xi\zeta}\Big)^{(q^f-1)/p} \equiv 1 \mod \mathfrak{q} \text{ for } k = 1, \dots, p-1.$$

We shall derive , by example, of this congruence that, for p sufficiently large, a very large number of primes should divide v. In an other hand we shall show that if q is any prime of order $f \mod p$ dividing $(u^p + v^p)$ then

$$(1-\zeta)^{(q^f-1)/p} \equiv p^{-(q^f-1)/p} \mod q,$$

and a result of same nature if q divides $u^p - v^p$, which reinforces strongly the first and second theorem of Furtwängler. The principle of proof relies on the p-Hilbert class field theory.

Keywords: Fermat's Last Theorem; cyclotomic fields; cyclotomic units; class field theory; Vandiver's and Furtwängler's theorems

MSC classification codes: 11D41; 11R18; 11R37

1 Introduction

Let $p > 3$ be a prime, $\zeta := e^{\frac{2\pi i}{p}}$, $K := \mathbb{Q}(\zeta)$ the pth cyclotomic number field, $\mathbb{Z}_K$ the ring of integers of K, and $\mathfrak{p} = (1-\zeta)\mathbb{Z}_K$ the prime ideal of $\mathbb{Z}_K$ over p. In [Gr2, Conj. 1.5], G. Gras has given a conjecture which implies Fermat's Last Theorem (FLT): we recall here this conjecture which will be called *Strong Fermat's Last Theorem conjecture* , denoted briefly $SFLT$.

Conjecture 1. *Let p be an odd prime, set $K = \mathbb{Q}(\zeta)$ and $\mathfrak{p} = (\zeta - 1)\,\mathbb{Z}[\zeta]$. Then the equation*

$$(u + v\,\zeta)\,\mathbb{Z}[\zeta] = \mathfrak{p}^{\delta}\,\mathfrak{w}_1^p$$

in coprime integers u, v, where δ is any integer ≥ 0 and $\mathfrak{w}_1$ is any integral ideal of K, has no solution for $p > 3$ except the trivial ones for which $u + v\,\zeta = \pm 1$, $\pm\zeta$, $\pm(1+\zeta)$, or $\pm(1-\zeta)$.

The cases $uv(u+v) \not\equiv 0 \mod p$, $uv \equiv 0 \mod p$, and $u + v \equiv 0 \mod p$ are called respectively the *first, second, and special case of* $SFLT$.

From some works of Furtwängler and Vandiver, Gras and I [GQ] have put the basis for a new cyclotomic approach to Fermat's Last Theorem by introducing some auxiliary fields of the form $\mathbb{Q}(\mu_{q-1})$ with prime $q \neq p$ in study of $SFLT$ equation.

In this article, we examine some particularities of the second case of $SFLT$ (hereinafter $SFLT2$). Without loss of generality, we choose the following formulation of $SFLT2$ in all the sequel:

Let $p > 3$ be a prime. The diophantine equation $\frac{u^p+v^p}{u+v} = w_1^p$ with $u, v, u+v, w_1 \in \mathbb{Z}\backslash\{0\}$, u, v coprime and $v \equiv 0 \mod p$ has no solution.

Observe that we assume $p > 3$ because, for $p = 3$, the diophantine equation $\frac{u^3+v^3}{u+v} = w_1^3$ has infinitely many solutions (u, v) where

$$(u, v) = (s^3 + t^3 - 3st^2, 3s^2t - 3st^2) = (s + tj)^3,$$

where s, t spans all $s, t \in \mathbb{Z},\ s + t \equiv 0 \mod 3,\ \gcd(s, t) = 1$ (see [GQ] remark 2.6).

Thus it is always assumed in the sequel, without further mention, that $p > 3$ and $p|v$. Observe that $SFLT2$ implies the second case $FLT2$ of FLT.

In the first subsection, we will fix some general notations, conventions, definitions, and in the second subsection p. 4, we will state the main results of the article.

1.1 General notations and definitions

Notations 1.

- Let $g := \mathrm{Gal}(K/\mathbb{Q})$, for $k \not\equiv 0 \mod p$ and $s_k : \zeta \to \zeta^k$ the $p-1$ distinct elements of g.

- Let $C\ell_K$, $C\ell$ and $C\ell_{[p]}$ be respectively the class group of K, the p-class group of K and the p-elementary class group of K. For any ideal $\mathfrak{a}$ of K, let us note $c\ell_K(\mathfrak{a})$ and $c\ell(\mathfrak{a})$ the class of $\mathfrak{a}$ in $C\ell_K$ and $C\ell$.

- For any integer $m > 0$, let $\Phi_m(X)$ be the mth cyclotomic polynomial and $\phi(m)$ the Euler indicator. For $a, b \in \mathbb{Z}\backslash\{0\}$, let us define $\Phi_m(a, b) := b^{\phi(m)}\Phi_m\left(\frac{a}{b}\right)$. Clearly $\Phi_m(a, b) \in \mathbb{Z}[a, b]$.

Definition 1. *A number $\alpha \in K^\times$ prime to p, such that $\alpha\mathbb{Z}_K$ is the pth power of an ideal, is called a pseudo-unit. The pseudo-unit α is p-primary (i.e. the extension $K(\sqrt[p]{\alpha})/K$ is unramified at $\mathfrak{p}$) if and only if α is congruent to a p-power $\mod \mathfrak{p}^p$, see [Gr2] lem 2.1.*

Definition 2. *A prime q is said p-principal if the class $c\ell_K(\mathfrak{q}_K) \in C\ell_K$ of any prime ideal $\mathfrak{q}_K$ of $\mathbb{Z}_K$ above q is the pth power of a class, which is equivalent to $\mathfrak{q}_K = \mathfrak{a}^p(\alpha)$, for an ideal $\mathfrak{a}$ of K and an $\alpha \in K^\times$. This contains the case where the class $c\ell_K(\mathfrak{q}_K)$ is of order coprime with p.* [1]

We assume that $SFLT2$ fails for (p, u, v); then $\gamma := u + v\zeta \in \mathbb{Z}_K$ is a p-primary pseudo-unit of $\mathbb{Z}_K$ since $\gamma \equiv u \mod p$ (a generalization of a result of Kummer given again in [Gr2], Theo. 2.2).

[1] Usually q is said p-principal if the class $c\ell_K(\mathfrak{q}_K)$ is of order coprime with p. We have adopted this generalization of the definition because we are interested in this article to some p-power residue symbols $\left(\frac{\eta}{\mathfrak{q}_K}\right)_K$ for η a p-primary unit of K. Class field theory implies that $\left(\frac{\eta}{\mathfrak{q}_K}\right)_K = 1$ even with this generalization.

Notations 2. *Let q be a prime number dividing $\Phi_n(u,v)$ with $q \not| n$ and $n = dp^r$ where d is prime to p and $r \geq 0$, which implies that $q \not| uv$ and $\frac{v}{u}$ is of order $n \mod q$ (see [GQ], Lem 2.11). We have*

$$\Phi_{dp^r}(u,v) := \prod (u\,\psi^i\,\zeta_r^j - v) \ \ \textit{for all} \ \ i \ \in (\mathbb{Z}/d\mathbb{Z})^\times \ \ \textit{and} \ \ j \ \in (\mathbb{Z}/p^r\mathbb{Z})^\times,$$

where $\psi := e^{\frac{2\pi i}{d}}$ and $\zeta_r := e^{\frac{2\pi i}{p^r}}$ (observe that the two previous definitions $\zeta := e^{\frac{2\pi i}{p}}$ and $\zeta_r := e^{\frac{2\pi i}{p^r}}$ imply that $\zeta_1 = \zeta$).

Let us fix the root of unity $\xi := \psi\,\zeta_r$. Let $L := \mathbb{Q}(\xi)$ and $M = LK = \mathbb{Q}(\xi,\zeta)$. Put $\mathfrak{q} = (q, u\,\xi - v)$ where $\mathfrak{q}$ is a prime ideal of L over q because we have assumed $q \not| n$. [2] *We denote by $\mathfrak{Q}$ any prime ideal of M over $\mathfrak{q}$ and by $\mathfrak{q}_K$ the prime ideal of K under $\mathfrak{Q}$.*

(i) If $r = 0$ then $L = \mathbb{Q}(\psi)$ and M is of degree $p-1$ over L.

(ii) If $r \geq 1$ then $M = L$ and $\mathfrak{Q} = \mathfrak{q}$.

Let us recall the definition of the pth power residue symbols in K and M with values in μ_p (see [GQ] definition 2.13).

Definition 3. *If $\alpha \in M$ is prime to $\mathfrak{Q}\,|\,\mathfrak{q}$ in M, then let $\bar\alpha$ be the image of α in the residue field $\mathbb{Z}_M/\mathfrak{Q} \simeq \mathbf{F}_{q^f}$; since $\zeta \in \mathbb{Z}_M$, the image $\bar\zeta$ of ζ is of order p (since $\zeta \not\equiv 1 \mod \mathfrak{Q}$) and we can put $\bar\alpha^\kappa = \bar\zeta^\mu$, $\kappa = \frac{q^f-1}{p}$, $\mu \in \mathbb{Z}/p\mathbb{Z}$, which defines the pth power residue symbol $\left(\frac{\alpha}{\mathfrak{Q}}\right)_M := \zeta^\mu$; this symbol is equal to 1 if and only if α is a local pth power at $\mathfrak{Q}$ (see [Gr1, I.3.2.1, Ex. 1]).*
With this definition, for any automorphism $\tau \in \mathrm{Gal}(M/\mathbb{Q})$ one obtains, from $\alpha^\kappa \equiv \zeta^\mu \mod \mathfrak{Q}$, $\tau\alpha^\kappa \equiv \tau\zeta^\mu \mod \tau\mathfrak{Q}$, thus $\tau\left(\frac{\alpha}{\mathfrak{Q}}\right)_M = \left(\frac{\tau\alpha}{\tau\mathfrak{Q}}\right)_M = \tau\zeta^\mu$.
If $\alpha \in K$, since $\mathfrak{q}_K\,|\,q$ in K splits totally in M/K, we have $\mathbb{Z}_K/\mathfrak{q}_K \simeq \mathbb{Z}_M/\mathfrak{Q}$ and $\left(\frac{\alpha}{\mathfrak{q}_K}\right)_K = \left(\frac{\alpha}{\mathfrak{Q}}\right)_M$ for any $\mathfrak{Q}\,|\,\mathfrak{q}_K$. In particular this implies $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = \zeta^\kappa$ (the symbol of ζ does not depend on the choice of $\mathfrak{q}_K\,|\,q$).

1.2 The main results

In the classical approach, the most part of the results on FLT for the exponent p are obtained by localization at p (Kummer, Mirimanoff, Wieferich, Vandiver and others) or by some properties of the p-class group of K (Eichler). There are less investigations with

[2] Observe that the prime ideal $\mathfrak{q}$ is fixed unambiguously by this choice of ξ.

localizations at primes $q \neq p$ (Sophie Germain, Vandiver, Wendt, Furtwängler, Krasner, Dénes and others).

Revisiting some ideas of Vandiver for FLT in [Va1, Va2] involving a systematic use of the pth power residue symbols $\left(\frac{a}{\mathfrak{Q}}\right)_M$ for $a \in M$ coprime with $\mathfrak{Q}$ (see definition 3), this article is a complement to the article [GQ] for localizations at primes $q \neq p$.

The main results of this article are : Assume that $SFLT2$ fails for (p, u, v). Let q be any odd prime coprime with puv, f the order of $q \mod p$, n the order of $\frac{v}{u} \mod q$, ξ a primitive nth root of unity, $\mathfrak{q}$ the prime ideal $(q, u\xi - v)$ of $\mathbb{Q}(\xi)$.

1. if q is *p-principal* and $n \neq 2p$ we prove (theorem 2.3) that

$$\Big(\frac{1+\xi\zeta^k}{1+\xi\zeta}\Big)^{(q^f-1)/p} \equiv 1 \mod \mathfrak{q} \text{ for } k = 1, \dots, p-1.$$

   We shall derive, by example, of this congruence that:

   - With a probabilistic estimate, more than half the primes $r < p^{p/5}$ of even degree mod p should divide v (remark 3).

   - If q of order $f \mod p$ divides $(u^p + v^p)$ then $(1-\zeta)^{(q^f-1)/p} \equiv p^{-(q^f-1)/p} \mod q$, (corollary 2.7 and 2.9).

   - If q of order $f \mod p$ divides $(u^p - v^p)$ then $(1-\zeta)^{(q^f-1)/p} \equiv 1 \mod q$, (corollary 2.7 and 2.8). These two last results reinforce strongly the first and second theorem of Furtwängler.

2. If $u + \zeta v \notin K^{\times p}$, then p is irregular and there exists an effective constant $C(p)$, depending only on p and smaller than Minkowski Bound, such that there exists at least one prime $q < C(p)$ satisfying q not dividing uv, q non p-principal and

$$\Big(\frac{\zeta^{-k^m}(1+\xi\zeta^k)}{\zeta^{-1}(1+\xi\zeta)}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for } k = 1, \dots, p-2,$$

   for a certain integer $m \not\equiv 0 \mod p$ and depending on q (theorem 2.13).

The principle of proofs of the article relies mainly on the p-Hilbert class field theory. Let us mention that, in this complement, we limited ourselves to the second case of $SFLT$ and principally to p-principal prime q. By opposite, we took also in account the case where p divides the order n of $\frac{v}{u} \mod q$, not examined in [GQ]. See also [Qu2] for some improvements of these results in the second case $FLT2$ of Fermat's Last Theorem.

2 The main theorem

At first, we give a definition and an elementary lemma independent of $SFLT$.

Definition 4. *Let $n = dp^r$, with d, p coprime and $r \geq 0$. Let ξ be a fixed primitive nth root of unity $\xi = \psi\zeta_r$ where $\psi := e^{\frac{2\pi i}{d}}$ and $\zeta_r := e^{\frac{2\pi i}{p^r}}$.*

For all $0 \leq k < p-1$, let us define[3]

$$\varepsilon_k := 1 + \xi\zeta^k.^4$$

Lemma 2.1.

a) If $k = 0$, $\varepsilon_0 = 1 + \xi$ is a cyclotomic unit of L except if $d = 1$ ($\varepsilon_0 = 2$) or $d = 2$ ($\varepsilon_0 = 0$).

b) Suppose that $0 < k < p-1$.

(i) If $d > 2$ then $\varepsilon_k = 1 + \xi\zeta^k$ is a cyclotomic unit.

(ii) If $d = 2$ then ε_k is not a cyclotomic unit and

– If $r \geq 1$ then $\varepsilon_k = 1 - \zeta_r^{1+kp^{r-1}} \in \mathbb{Z}[\zeta_r]$ with $\varepsilon_k\mathbb{Z}[\zeta_r] = \mathfrak{p}_r$ where $\mathfrak{p}_r$ is the prime ideal of $\mathbb{Z}[\zeta_r]$ above p.

– If $r = 0$ then $\varepsilon_k = 1 - \zeta^k$ with $\varepsilon_k\mathbb{Z}_K = \mathfrak{p}$.

(iii) If $d = 1$ then ε_k is a cyclotomic unit and

– If $r \geq 1$ then $\varepsilon_k = 1 + \zeta_r^{1+kp^{r-1}}$.

– If $r = 0$ then $\varepsilon_k = 1 + \zeta^k$.

Proof. Left to the reader. □

The following lemma using Hilbert class field theory for K plays a central role in the article.

Lemma 2.2. *Suppose that $SFLT2$ fails for (p, u, v). Let $q \not| \, puv$ be a p-principal prime, n the order of $\frac{v}{u} \mod q$, $\xi := e^{\frac{2\pi i}{n}}$ and $\mathfrak{q}$ the prime ideal $(u\xi - v, q)$ of $\mathbb{Z}_L$. Then*

$$\Big(\frac{1+\xi\zeta^k}{\mathfrak{Q}}\Big)_M = \Big(\frac{u}{\mathfrak{q}_K}\Big)_K^{-1} \text{ for all } k = 1, \dots, p-2 \text{ and all } \mathfrak{Q}|\mathfrak{q} \text{ with } \mathfrak{q}_K \text{ under } \mathfrak{Q}.^5$$

[3] The reason why $k = p-1$ is discarded will be explained in remark 1 after the lemma 2.2.
[4] ε_k is used with this meaning in the sequel of the article.
[5] Observe that $\big(\frac{u}{\mathfrak{q}_K}\big)_K$ does not depend on k and recall that $\mathfrak{Q} = \mathfrak{q}$ if $r > 0$.

Proof. Let us choose one $\mathfrak{Q}$ over $\mathfrak{q}$ with $\mathfrak{q}_K$ under $\mathfrak{Q}$ and observe what happens when k varies thorough $1,\dots,p-1$:

- We have $u\xi - v \equiv 0 \mod \mathfrak{q}$, so $u\xi - v \equiv 0 \mod \mathfrak{Q}$, hence with $\gamma := u+\zeta v$, we get $s_k(\gamma) = u+\zeta^k v \equiv u(1+\xi\zeta^k) \equiv u\varepsilon_k \mod \mathfrak{Q}$ for $k=1,\dots,p-1$.

- We obtain $\left(\frac{s_k(\gamma)}{\mathfrak{Q}}\right)_M = \left(\frac{u}{\mathfrak{Q}}\right)_M \left(\frac{\varepsilon_k}{\mathfrak{Q}}\right)_M$, so $\left(\frac{s_k(\gamma)}{\mathfrak{q}_K}\right)_K = \left(\frac{u}{\mathfrak{q}_K}\right)_K \left(\frac{\varepsilon_k}{\mathfrak{Q}}\right)_M$.

- The numbers $s_k(\gamma)$ are p-primary pseudo-units, which implies $\left(\frac{s_k(\gamma)}{\mathfrak{q}_K}\right)_K = 1$ for all $k \not\equiv 0 \mod p$ from the decomposition of primes in Hilbert class fields because, by assumption, q is p-principal.

- We can reiterate the same reasoning for all $\mathfrak{Q}$ over $\mathfrak{q}$.

□

Remark 1. We explain why we can discard the value $k=p-1$ of the index k. The value $k=p-1$ is excluded because ε_k would be null if and only if $d=2, r=1$ and $k=p-1$. This particular case shall be directly examined in the corollary 2.9. For all the other (d,r,k), $1 \le k \le p-1$ with $\varepsilon_k \neq 0$, we show now that it is always possible to express $\left(\frac{1+\xi\zeta^{p-1}}{\mathfrak{Q}}\right)_M$ in function of $\left(\frac{1+\xi\zeta^k}{\mathfrak{Q}}\right)_M$, $k=1,\dots,p-2$: we start from

$$u(1+\xi\zeta^j) \equiv s_j(\gamma) \mod \mathfrak{q}, \text{ for } j=1,\dots,p-1,$$

where $1+\xi\zeta^j$ is always nonzero, therefore

$$u^{p-1}\prod_{j=1}^{p-1}(1+\xi\zeta^j) \equiv N_{K/\mathbb{Q}}(\gamma) = w_1^p \mod \mathfrak{q},$$

so

$$\left(\frac{u^{p-1}(1+\xi\zeta)\dots(1+\xi\zeta^{p-2})(1+\xi\zeta^{p-1})}{\mathfrak{Q}}\right)_M = 1 \text{ for all } \mathfrak{Q}|\mathfrak{q}$$

so, from lemma 2.2 applied for all $1 \le k \le p-2$ we get $\left(\frac{u(1+\xi\zeta^{p-1})}{\mathfrak{Q}}\right)_M = 1$, and thus

$$\left(\frac{1+\xi\zeta^{p-1}}{\mathfrak{Q}}\right)_M = \left(\frac{1+\xi\zeta^k}{\mathfrak{Q}}\right)_M, \text{ for all } k=1,\dots,p-2.$$

2.1 The general case

Our main results on $SFLT2$ are a direct consequence of the lemma 2.2 dealing with the decomposition of $\mathfrak{Q}$ in a certain Kummer p-extension defined from the Vandiver's cyclotomic units. They will follow from:

Theorem 2.3. *Assume that $SFLT2$ fails for (p,u,v). Let $q \not| puv$ be a p-principal prime, n the order of $\frac{v}{u} \mod q$, $\xi := e^{\frac{2\pi i}{n}}$ and $M := \mathbb{Q}(\xi,\zeta)$. For all $0 \leq k < p-1$, let $\varepsilon_k := 1+\xi\zeta^k$ and $\mathfrak{q}$ be the prime ideal $(q, u\,\xi - v)$ of $\mathbb{Z}[\xi]$ over q.*

Then all the prime ideals $\mathfrak{Q}$ of $\mathbb{Z}[\xi,\zeta]$ over $\mathfrak{q}$ split totally [6] *in the Kummer extension*

$$M\Big(\sqrt[p]{<\varepsilon_k\varepsilon_1^{-1}>_{k=1,\dots,p-2}}\Big)/M.$$

Proof. It is a reformulation of the previous lemma 2.2 where $\big(\frac{\varepsilon_k}{\mathfrak{Q}}\big)_M = \big(\frac{\varepsilon_1}{\mathfrak{Q}}\big)_M$, for $k = 1,\dots,p-2$. $\square$

Corollary 2.4. *Assume that $SFLT2$ fails for (p,u,v). Let $q \not| puv$ be a p-principal prime, n the order of $\frac{v}{u} \mod q$, $\xi := e^{\frac{2\pi i}{n}}$ and $\mathfrak{q}$ be the prime ideal $(q, u\,\xi - v)$ of $\mathbb{Z}[\xi]$ over q.*

If $n \neq 2p$ then

$$\Big(\frac{1+\xi\zeta^k}{1+\xi\zeta}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for all } k = 1,\dots,p-1. \tag{1}$$

Proof.

1. If $p \mid n$ then we have $\mathfrak{q} = \mathfrak{Q}$ and, from theorem 2.3, we get for the pair $(\mathfrak{q}_K, \mathfrak{Q})$ with $\mathfrak{q}_K$ under $\mathfrak{Q}$

$$\Big(\frac{1+\xi\zeta^k}{1+\xi\zeta}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for all } \ k = 1,\dots,p-1.$$ [7]

2. If $p \not| n$ then for all $k = 1,\dots,p-1$, we have

$$\Big(\frac{1+\xi\zeta^k}{1+\xi\zeta}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{Q} \text{ for all } \mathfrak{Q} \mid \mathfrak{q},$$

because for each triple $(\mathfrak{q}_K, \mathfrak{q}, \mathfrak{Q})$ with $\mathfrak{Q}$ over $\mathfrak{q}$ and $\mathfrak{q}_K$ under $\mathfrak{Q}$ we have $\big(\frac{u}{\mathfrak{q}_K}\big)_K \big(\frac{1+\xi\zeta^k}{\mathfrak{Q}}\big)_M = \big(\frac{u}{\mathfrak{q}_K}\big)_K \big(\frac{1+\xi\zeta}{\mathfrak{Q}}\big)_M = 1.$

$\square$

Remark 2.

[6] Recall that $\mathfrak{Q} = \mathfrak{q}$ if $p \mid n$.

[7] In fact, we can consider all $k = 1,\dots,p-1$ and not only $k = 1,\dots,p-2$ from remark 1 except in the case where $n = 2p$ which is examined directly in corollary 2.9.

1. The relation (1) is equivalent to : for all prime ideals $\mathfrak{Q}$ of $M = \mathbb{Q}(\xi, \zeta)$ over $\mathfrak{q}$ then $\mathfrak{Q}$ splits totally in the p-Kummer extension $M\big(\sqrt[p]{< (1+\xi\zeta^k)/(1+\xi\zeta) >_{k=1,\dots,p-2}}\big)/M$.

2. Observe that lemma 2.2 implies similarly that:

   (a) if $\big(\frac{u}{\mathfrak{q}_K}\big)_K = 1$ then all the prime ideals $\mathfrak{Q}$ of $\mathbb{Z}[\xi,\zeta]$ dividing $\mathfrak{q}$ split totally in the Kummer extension $M\big(\sqrt[p]{< (1+\xi\zeta^k >_{k=1,\dots,p-2}}\big)/M$.

   (b) if $\big(\frac{u}{\mathfrak{q}_K}\big)_K \neq 1$ then all the prime ideals $\mathfrak{Q}$ of $\mathbb{Z}[\xi,\zeta]$ dividing $\mathfrak{q}$ are inert in the Kummer extension $M\big(\sqrt[p]{< (1+\xi\zeta^k >_{k=1,\dots,p-2}}\big)/M$.

Corollary 2.5. *Assume that Vandiver conjecture holds for p and that $SFLT2$ fails for (p,u,v). Let $q \neq p$ be a prime whose order $f \mod p$ is even and such that p does not divide $\frac{q^f-1}{p}$. Let n be the order of $\frac{v}{u} \mod q$, $\xi := e^{\frac{2\pi i}{n}}$ and $\mathfrak{q}$ be the prime ideal $(q, u\,\xi - v)$ of $\mathbb{Z}[\xi]$ over q. If $n \neq 2p$ then, either*

$$\Big(\frac{1+\xi\zeta^k}{1+\xi\zeta}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for all } k = 1,\dots,p-1, \tag{2}$$

or q divides v.

Proof. From the first theorem of Furtwängler for SFLT, see [GQ] cor 2.15 (i) and the assumption $\frac{q^f-1}{p} \not\equiv 0$, we derive that q does not divide u. The order of $q \mod p$ is even, so $\big(\frac{u}{\mathfrak{q}_K}\big)_K = 1$ and $\mathfrak{q}_K$ is p-principal because Vandiver's conjecture holds for p. Then we apply corollary 2.4. $\square$

Remark 3.

1. If $SFLT2$ fails for (p,u,v) with $p|v$ and if the p-principal prime $q < p$, the probability is very small, for the ideal $\mathfrak{q}$ of L over q, to split totally in the Kummer extension $M\Big(\sqrt[p]{< \varepsilon_k\varepsilon_1^{-1} >_{k=1,\dots,p-1}}\ \Big)/M$: let p^δ be the degree of this Kummer extension; the probability estimate that $\mathfrak{q}$ split totally in this extension satisfies

$$\mathcal{P} \leq \frac{\phi(n)}{p^\delta} \leq \frac{\phi(q-1)}{p^\delta}).$$

2. As a consequence, if $SFLT2$ failed for (p,u,v) with $p|v$ sufficiently large, these probability estimates suggest that the integer $|v|$ should be a *very large integer* with a very large number of p-principal primes $q|v$ with $\kappa \not\equiv 0 \mod p$. As an example, apply

cor. 2.5 for $p = 491$. Assume that $SFLT2$ fails for $p = 491$. The primes $q < p$ of even degree $\mod p$ with $\kappa \not\equiv 0 \mod p$ are : $2, 7, 19, 23, 29, 47, 53, 59, 67, 73, 89, 103, 109, 113, 137, 149, 151, 157, 167, 173, 191, 193, 193, 211, 251, 271, 281, 283, 307, 311, 313, 317, 337, 347, 353, 359, 367, 373, 383, 397, 421, 431, 433, 439, 443, 439, 479, 487$. For these primes, we have $\mathcal{P} < \frac{1}{p^\delta - 1}$ is very small.

We see that there is a large number of primes dividing v, a fortiori if we consider all such primes of even order $\mod p$ for $q < p^\nu$ with for instance $\nu < \delta - 2$. It is reasonable to think that for p sufficiently large we have $\delta < \frac{p}{4}$, so we can take $\nu < \frac{p}{5}$ to assert that *more than half of all the primes* $q < p^{\frac{p}{5}}$ *of even order* $\mod p$ *should not satisfy (2) and so should divide* v. We have not found in the FLT literature that $x^p + y^p + z^p = 0$ with $p|y$ should imply that y must have a so very large number of small prime factors. This observation could bring some tools for another diophantine tackling of $SFLT2$ and $FLT2$, for instance in the spirit of Thue, see Ribenboim [Rib1] (3B) p. 233 or Baker's linear form of logarithm or others. It is possible to formulate a corollary with an assumption independent of the values (u, v) of any possible counter-example which should imply that $SFLT2$ holds for p:

Corollary 2.6. *Let $p > 3$ be a prime. Assume that there exist infinitely many primes q such that, for $\xi_{q-1} := e^{\frac{2\pi i}{q-1}}$ and $L := \mathbb{Q}(\xi_{q-1})$, there is no prime ideal $\mathfrak{q}$ of L such that*

$$\Big(\frac{1 + \xi_{q-1}\zeta^k}{1 + \xi_{q-1}\zeta}\Big)^{\frac{q^f - 1}{p}} \equiv 1 \mod \mathfrak{q} \quad \textit{for all } k = 1, \dots, p-1.$$

Then $SFLT2$ holds for p.

Proof. Suppose that $SFLT2$ fails for (p, u, v). There are infinitely many q, so there is at least one q such that $uv \not\equiv 0 \mod q$. Let $n := q - 1$, then $u^n - v^n \equiv 0 \mod q$. Let $\xi := e^{\frac{2\pi i}{n}}$ and $L = \mathbb{Q}(\xi)$. There exists a prime ideal $\mathfrak{q}$ of $\mathbb{Z}_L$ such that $u\xi_{q-1} - v \equiv 0 \mod \mathfrak{q}$. Then, by corollary 2.5, we should have $\Big(\frac{1+\xi_{q-1}\zeta^k}{1+\xi_{q-1}\zeta}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q}$ for all $k = 1, \dots, p - 2$, contradicting the assumptions made on q. □

The existence of an infinity of primes q satisfying assumptions of corollary 2.6 is an *open question* because $\frac{\phi(q-1)}{p^{p-1}} \to \infty$ when $q \to \infty$.

2.2 The case $n \in \{p, 1, 2p, 2\}$

In this subsection, we suppose that $SFLT2$ fails for (p, u, v) and we apply the lemma 2.2 in fixing $n \in \{p, 1, 2p, 2\}$ to derive some strong properties of all the p-principal primes q

dividing $\Phi_n(u,v)$ for these values of n. Observe that we have $M = K$ in all these cases.

2.2.1 The two cases $n = p$ and $n = 1$.

The reunion of these two cases allows us to investigate the properties of all the p-principal primes q dividing $u^p - v^p$.

Corollary 2.7. *Case $n = p$: suppose that $SFLT2$ fails for (p,u,v). If q is a p-principal prime dividing $\frac{u^p-v^p}{u-v}$ then*

$$q \equiv 1 \mod p^2 \text{ and } (1+\zeta)^{(q-1)/p} \equiv u^{(q-1)/p} \equiv v^{(q-1)/p} \equiv 2^{(q-1)/p} \equiv 1 \mod q.$$

Proof. Here $\xi = \zeta$, $u\zeta - v \equiv 0 \mod \mathfrak{q}$, $\varepsilon_k = 1 + \zeta^{k+1}$, $M = L = K$ and $\mathfrak{q} = \mathfrak{Q} = \mathfrak{q}_K$, so $\left(\frac{1+\zeta^{k+1}}{\mathfrak{q}_K}\right)_K = \left(\frac{u}{\mathfrak{q}_K}\right)_K^{-1}$ for all $k = 1, \ldots, p-2$ from lemma 2.2. It follows that $\left(\frac{1+\zeta^2}{\mathfrak{q}_K}\right)_K = \left(\frac{1+\zeta^{-2}}{\mathfrak{q}_K}\right)_K$, which implies that $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = 1$, thus $q \equiv 1 \mod p^2$, observing that $q \equiv 1 \mod p$.

From $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = 1$, we get $\left(\frac{1+\zeta}{\mathfrak{q}_K}\right)_K = \left(\frac{1+\zeta^{p-1}}{\mathfrak{q}_K}\right)_K$, so $\left(\frac{1+\zeta^j}{\mathfrak{q}_K}\right)_K = \left(\frac{u}{\mathfrak{q}_K}\right)_K^{-1}$, for all $j = 1, \ldots, p-1$. Thus $\left(\frac{1+\zeta}{\mathfrak{q}_K}\right)_K = \ldots = \left(\frac{1+\zeta^{p-1}}{\mathfrak{q}_K}\right)_K$. Therefore $\left(\frac{N_{K/\mathbb{Q}}(1+\zeta)}{\mathfrak{q}_K}\right) = \left(\frac{u^{-1}}{\mathfrak{q}_K}\right)_K^{p-1} = 1$, so $\left(\frac{u}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K = 1$, and gathering these results we get

$$\left(\frac{1+\zeta}{\mathfrak{q}_K}\right)_K = \ldots = \left(\frac{1+\zeta^{p-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{u}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K = 1.$$

From $u\zeta - v \equiv 0 \mod \mathfrak{q}_K$, we have $w_1^p = \frac{u^p+v^p}{u+v} \equiv \frac{2u^p}{u(1+\zeta)} \mod \mathfrak{q}_K$, so $\left(\frac{2}{\mathfrak{q}_K}\right)_K = 1$, and finally

$$\left(\frac{2}{\mathfrak{q}_K}\right)_K = \left(\frac{1+\zeta}{\mathfrak{q}_K}\right)_K = \cdots = \left(\frac{1+\zeta^{p-1}}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K = \left(\frac{u}{\mathfrak{q}_K}\right)_K = 1.$$

By conjugation by s_ℓ, we get $\left(\frac{1+\zeta}{s_\ell(\mathfrak{q}_K)}\right)_K = 1$ for any $\ell \not\equiv 0 \mod p$, thus

$$(1+\zeta)^{(q-1)/p} \equiv 1 \mod q.$$

□

Corollary 2.8. *Case $n = 1$: suppose that $SFLT2$ fails for (p,u,v). If q is a p-principal prime of order $f \mod p$ and q divides $u - v$ then we have:*

$$q^f \equiv 1 \mod p^2 \text{ and } u^{(q^f-1)/p} \equiv v^{(q^f-1)/p} \equiv (1+\zeta)^{(q^f-1)/p} \equiv 2^{(q^f-1)/p} \equiv 1 \mod q.$$

Proof. Here $\varepsilon_k = 1+\zeta^k$, $M = K$ and $L = \mathbb{Q}$. The proof is very similar to the case $n = p$ corollary 2.7 starting here from the relation

$$u + \zeta^j v \equiv u(1+\zeta^j) \mod q, \tag{3}$$

for all $j \not\equiv 0 \mod p$ (instead of a congruence $\mod \mathfrak{q}_K$), observing that the degree of q mod p can be here greater than 1. We have $N_{K/\mathbb{Q}}(1+\zeta) = 1$ which implies that $\left(\frac{u}{\mathfrak{q}_K}\right)_K = 1$ and then $\frac{u^p+v^p}{u+v} = w_1^p \equiv \frac{2^p u^p}{2u} \mod q$ implies $\left(\frac{2}{\mathfrak{q}_K}\right)_K = 1$. □

Remark 4. Corollaries 2.7 and 2.8 imply that all the p-principal primes q dividing $u^p - v^p$ satisfy $q^f \equiv 1 \mod p^2$, which brings a new generalization of the second Furtwängler's theorem in $SFLT2$ context obtained for the only primes q dividing $u - v$ in [GQ] cor. 2.16. In the other hand, the fact that $(1+\zeta)^{\frac{q^f-1}{p}} \equiv 1 \mod q$ for all $q \mid u^p - v^p$ is new.

2.2.2 The two cases $n = 2p$ and $n = 2$

The reunion of these two corollaries of the theorem 2.3 allows us to investigate all the p-principal primes q dividing $u^p + v^p$ at the *core* of the $SFLT2$ equation. We need to modify slightly the method to take into account the only values k with $\mathfrak{q}_K$ co-prime with $u + \zeta^k v$.

Corollary 2.9. *Case $n = 2p$: suppose that $SFLT2$ fails for (p, u, v). If q is a p-principal prime dividing $\frac{u^p+v^p}{u+v}$ then*

$$q \equiv 1 \mod p^2 \text{ and } (1-\zeta)^{\frac{q-1}{p}} \equiv p^{-\frac{q-1}{p}} \equiv u^{-\frac{q-1}{p}} \equiv v^{-\frac{q-1}{p}} \mod q.$$

Proof. Here, we have $M = K = L$ and $\xi = -\zeta$ which implies that $v \equiv -\zeta u \mod \mathfrak{q} = \mathfrak{q}_K$, thus

$$s_k(u+\zeta v) = u + \zeta^k v = s_k(\gamma) \equiv u(1-\zeta^{k+1}) \mod \mathfrak{q}, \;\; k = 1, \dots p-2.$$

We obtain $\left(\frac{u}{\mathfrak{q}_K}\right)_K \left(\frac{1-\zeta^{k+1}}{\mathfrak{q}_K}\right)_K = 1$, for $k \not\equiv p-1 \mod p$ from lemma 2.2, therefore $\left(\frac{1-\zeta^2}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta^{p-2}}{\mathfrak{q}_K}\right)_K$, so $\left(\frac{\zeta}{\mathfrak{q}_K}\right)_K = 1$ and $q \equiv 1 \mod p^2$, which implies that $\left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta^{p-1}}{\mathfrak{q}_K}\right)_K$. Gathering these results, we get

$$\left(\frac{1-\zeta}{\mathfrak{q}_K}\right)_K = \cdots = \left(\frac{1-\zeta^{p-1}}{\mathfrak{q}_K}\right)_K,$$

by multiplication we get $\left(\frac{u^{p-1}}{\mathfrak{q}_K}\right)_K \left(\frac{p}{\mathfrak{q}_K}\right)_K = 1$ and finally:

$$\left(\frac{u}{\mathfrak{q}_K}\right)_K = \left(\frac{v}{\mathfrak{q}_K}\right)_K = \left(\frac{p}{\mathfrak{q}_K}\right)_K = \left(\frac{1-\zeta^j}{\mathfrak{q}_K}\right)_K^{-1}, \;\; \text{for all } j \not\equiv 0 \mod p.$$

We get $\left(\frac{(1-\zeta^j)p}{\mathfrak{q}_K}\right)_K = 1$ for all $j \not\equiv 0 \mod p$, so $((1-\zeta)p)^{\frac{q-1}{p}} \equiv 1 \mod q$ and finally $(1-\zeta)^{(q-1)/p} \equiv p^{-\frac{q-1}{p}} \mod q$. $\square$

Corollary 2.10. *Case $n = 2$: suppose that $SFLT2$ fails for (p, u, v). If q is a p-principal prime dividing $u + v$ of degree $f \mod p$ then*

$$q^f \equiv 1 \mod p^2 \text{ and } (1-\zeta)^{\frac{q^f-1}{p}} \equiv p^{-\frac{q^f-1}{p}} \equiv u^{-\frac{q^f-1}{p}} \mod q \equiv v^{-\frac{q^f-1}{p}} \mod q.$$

Proof. Here, $\varepsilon_j = 1 - \zeta^j$ for $j \not\equiv 0 \mod p$, $M = K$ and $L = \mathbb{Q}$. In that case, we get $\left(\frac{u}{\mathfrak{q}_K}\right)_K \left(\frac{1-\zeta^j}{\mathfrak{q}_K}\right)_K = 1$ for all $j \not\equiv 0 \mod p$. The end of the proof is similar to that of corollary 2.9. $\square$

Remark 5. Corollaries 2.9 and 2.10 imply that all the p-principal primes q dividing $u^p + v^p$ satisfy $q^f \equiv 1 \mod p^2$, which brings a generalization of the first Furtwängler's theorem in the $SFLT2$ context obtained for the only primes q dividing $u + v$ in [GQ] cor. 2.15. In the other hand, the fact that $(1-\zeta)^{\frac{q^f-1}{p}} \equiv p^{-\frac{q^f-1}{p}} \mod q$ for the primes dividing $u^p + v^p$ is new.

2.3 The case $u + \zeta v \notin K^{\times p}$

In this subsection, we assume that $SFLT2$ fails for (p, u, v) with $p \mid v$ and $u + \zeta v \notin K^{\times p}$. It follows that p is irregular, if not the p-primary pseudo-unit $u + \zeta v$ should belong to $K^{\times p}$, see for instance Gras [Gr2] thm 2.2.

Lemma 2.11. *Let $q \neq p$ be a prime number and $\mathfrak{q}_K$ any prime ideal of $\mathbb{Z}_K$ over q. If q divides u (resp v) then $\left(\frac{v}{\mathfrak{q}_K}\right)_K = 1$ (resp. $\left(\frac{u}{\mathfrak{q}_K}\right)_K = 1$).*

Proof. We have $N_{K/\mathbb{Q}}(u + v\zeta) = \frac{u^p+v^p}{u+v} = w_1^p$, where $N_{K/\mathbb{Q}}(\mathfrak{w}_1) = w_1$; so $q \mid v$ implies that $u^{p-1} \equiv w_1^p \pmod q$, which leads to $\left(\frac{u}{\mathfrak{q}_K}\right)_K = 1$. Similar proof starting from $q \mid u$. $\square$

Let $\mathcal{S}$ be a finite set of non p-principal primes q such that the set of p-classes $c\ell(\mathfrak{q}_K) \in C\ell$ of the prime ideals $\mathfrak{q}_K$ of K over q generates the p-elementary p-class group $C\ell_{[p]}$ of K. Let us note Q_p the greatest prime $q \in \mathcal{S}$. Let the Minkowski Bound of K given by

$$\mathcal{B}_p := \left(\frac{4}{\pi}\right)^{(p-1)/2} \frac{(p-1)!}{(p-1)^{p-1}} \sqrt{p^{p-2}}.$$

With these definitions, we can always choose a set $\mathcal{S}$ such that Q_p be smallest possible with $Q_p \leq \mathcal{B}_p$. Under the General Riemann Hypothesis GRH, we know that the whole ideal class group of K is generated by the set of prime ideals $\mathfrak{l}$ with

$$N_{K/\mathbb{Q}}(\mathfrak{l}) < B := 12(\log \Delta_K)^2, \tag{4}$$

where Δ_K is the absolute discriminant of K (see [BDF]). Under GRH, we have generally $Q_p \ll \mathcal{B}_p$ (where here $\ll$ means *very small compare to*) as soon as p is large.

Lemma 2.12. *Suppose that $u + \zeta v \notin K^{\times p}$. Then there exists at least one prime $q \in \mathcal{S}$ such that $uv \not\equiv 0 \pmod q$.*

Proof. Let γ be a pth root of $u + \zeta v$, $\gamma := \sqrt[p]{u+\zeta v}$. Let H_1 be the p-elementary Hilbert class field of K (so that $\mathrm{Gal}(H_1/K) \simeq C\ell_{[p]}$). Let N_1 be a subextension of H_1 such that H_1 is the direct compositum of N_1 and $K(\sqrt[p]{\gamma})$ over K.

Therefore there exists at least one prime $q \in \mathcal{S}$ such that the Frobenius of all the prime ideals $\mathfrak{q}_K$ over q in H_1/K are of order p and fix N_1, so that their restriction to $K(\sqrt[p]{\gamma})/K$ are of order p. Thus $\left(\frac{u+\zeta v}{\mathfrak{q}_K}\right)_K \neq 1$.

(i) If $q \mid v$, we get a contradiction with lemma 2.11, so $v \not\equiv 0 \mod q$.

(ii) If $q \mid u$ we have $\left(\frac{u+\zeta v}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta v}{\mathfrak{q}_K}\right)_K = \left(\frac{\zeta}{\mathfrak{q}_K}\right)_K$ because $\left(\frac{v}{\mathfrak{q}_K}\right)_K = 1$ from Lemma 2.11, thus $\left(\frac{u+\zeta v}{\mathfrak{q}_K}\right)_K = 1$ since $\kappa \equiv 0 \pmod p$ from the first Furtwangler's theorem for SFLT (see [GQ, Corollary 2.15]), which brings also a contradiction with $\left(\frac{u+\zeta v}{\mathfrak{q}_K}\right)_K \neq 1$. Therefore $u \not\equiv 0 \pmod q$. $\square$

Definition 5. For a definition of the character of Teichmüller ω of $Gal(K/\mathbb{Q})$, see for instance [GQ] definition 2.8. Let us consider the characters $\chi_i = \omega^i$, $1 \leq i \leq p-1$. Let $\mathcal{E}$ be the group of p-primary pseudo-units of K seen as a $\mathbb{F}_p[g]$-module, and the χ_i-components $\mathcal{E}_i := \mathcal{E}^{e_{\chi_i}}$ of $\mathcal{E}$. The components $\mathcal{E}_i$ are not all trivial because p is irregular.

Theorem 2.13. *Suppose that $SFLT2$ fails for (p,u,v) with $u + \zeta v \notin K^{\times p}$. Then p is irregular and there exists at least one non p-principal prime $q \in \mathcal{S}$ such that:*

1. *We have $q \not| \, uv$.*
2. *n being the order of $\frac{v}{u} \mod q$, $\xi := e^{\frac{2\pi i}{n}}$, $\mathfrak{q}$ the prime ideal $(u\xi - v, q)$ of $\mathbb{Z}[\xi]$ over q, we have*
$$\left(\frac{\zeta^{-k^m}(1+\xi\zeta^k)}{\zeta^{-1}(1+\xi\zeta)}\right)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for } k = 1, \ldots, p-2,$$
for a certain $m \in (\mathbb{Z}/p\mathbb{Z})^\times$.

Proof.

1. p is irregular as seen above. From lemma 2.12 it is possible to choose $q \in \mathcal{S}$ with $uv \not\equiv 0 \mod p$.

2. The pseudo-unit $\gamma = \sqrt[p]{u+\zeta v}$ is not a pth power, hence in the decomposition $\gamma = \prod_{\chi_i} \gamma^{e_{\chi_i}}$ on the p-1 characters $\chi_i,\ i = 1, \dots, p-1$, there exists at least one $i = m$ such that the pseudo-unit $\gamma^{e_{\chi_m}}$ be not a p-power. Let us name γ_m this idempotent.

   γ_m is a p-primary pseudo-unit; from Hilbert's class field theory and lemma 2.12 applied with H_1 and γ_m, it is possible to choose one $\mathfrak{q}_K \in \mathcal{S}$ such that

   $$\left(\frac{\gamma_m}{\mathfrak{q}_K}\right)_K = \zeta^{w_m} \text{ with } w_m \not\equiv 0 \mod p \text{ and } \left(\frac{\gamma_i}{\mathfrak{q}_K}\right)_K = 1 \text{ for all } \ i \neq m.$$

3. Here the extension $M(\sqrt[p]{\gamma_m})$ is Galois on $\mathbb{Q}$ because its Galois group acts in letting globally unvarying the radical, when raising to a power prime to p, by use of the idempotent. We can always change $\mathfrak{q}_K$ in acting by conjugation to obtain $w_m = 1$ and so

   $$\left(\frac{\gamma}{\mathfrak{q}_K}\right)_K = \left(\frac{\gamma_m}{\mathfrak{q}_K}\right)_K = \zeta.$$

4. From $s_k(\gamma) = u + \zeta^k v$ for $k = 1, \dots, p-2$ and $u\xi - v \equiv 0 \mod \mathfrak{q}$ we get

   $$s_k(\gamma) \equiv u\varepsilon_k \mod \mathfrak{q},$$

   where $\varepsilon_k = 1 + \xi\zeta^k$, so, as in lemma 2.2, $s_k(\gamma) \equiv u\varepsilon_k \mod \mathfrak{Q}$ for all $\mathfrak{Q}$ over $\mathfrak{q}$ and

   $$\left(\frac{s_k(\gamma)}{\mathfrak{q}_K}\right)_K = \left(\frac{u\varepsilon_k}{\mathfrak{Q}}\right)_M = \left(\frac{s_k(\gamma_m)}{\mathfrak{q}_K}\right)_K = \zeta^{k^m}$$

   because γ_m is an idempotent, so

   $$\left(\frac{u(1+\xi\zeta^k)}{\mathfrak{Q}}\right)_M = \zeta^{k^m},$$

   and also

   $$\left(\frac{u(1+\xi\zeta)}{\mathfrak{Q}}\right)_M = \zeta,$$

   which leads to

   $$\left(\frac{\zeta^{-k^m}(1+\xi\zeta^k)}{\zeta^{-1}(1+\xi\zeta)}\right)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for } k = 1, \dots, p-1.$$

$\square$

This theorem leads us to set the following *criterion* depending only on p [8] to reduce the SFLT2 equation to the form $u+\zeta v \in K^{\times p}$ for the irregular prime p:

Corollary 2.14. *Let p be an odd irregular prime. Assume that SFLT2 fails for p and that there is no integer $1 \leq m \leq p-1$, no prime $\mathfrak{q}$ in $\mathbb{Z}[\xi_{q-1}]$ over a prime $q \in \mathcal{S}$ with ξ_{q-1} a $(q-1)$th primitive root of unity such that*

$$\Big(\frac{\zeta^{-km}(1+\xi_{q-1}\zeta^k)}{\zeta^{-1}(1+\xi_{q-1}\zeta)}\Big)^{\frac{q^f-1}{p}} \equiv 1 \mod \mathfrak{q} \text{ for } k=1,\dots,p-2.$$

Then the solution(s) of the $SFLT2$ equation take(s) the reduced form $u+\zeta v \in K^{\times p}$.

Remark 6. Suppose, as an example, that $SFLT2$ fails for p and that $p \| \mathcal{C}\ell_K$ class group of K, which implies that $Card(\mathcal{S})=1$. Under GRH, from [BDF], the definition of $\mathcal{S}$ should imply that $Q_p < 12(p-2)^2(log\ p)^2$. For one $q \in \mathcal{S}$, the probability estimate $\mathcal{P}$ that $\mathfrak{q}$ split totally in the Kummer extension

$$M\Big(\sqrt[p]{<((1+\xi\zeta^k)\zeta^{-km})/((1+\xi\zeta)\zeta^{-1})>_{k=1,\dots,p-2}}\ \Big)/M,$$

of degree p^δ are $\mathcal{P} \leq \frac{Q_p}{p^\delta}$, because $\phi(q) \leq Q_p$ for $q \in \mathcal{S}$. Note that often, and perhaps for all irregular primes $p > 10^3$, we have $\delta > \frac{p}{4}$ and, under GRH, we have $Q_p < p^3$, so

$$\mathcal{P} < \frac{1}{p^{\frac{p}{4}-3}}.$$

Acknowledgments: I would like to thank Georges Gras and Preda Mihailescu for pointing out some errors and suggesting some improvements for the content and form of the article.

References

[BDF] K. Belabas, F. Diaz Y Diaz, and E. Friedman, *Small generators of the ideal class group*, Mathematics of Computation 77, 262 (2008) 1185–1197.

[8] We use intentionally the term *criterion* to indicate that corollary 2.14 allows us (at least theoretically) in a finite number of arithmetic computations to determine if, for p given, the SFLT2 equation can be reduced to the form $u+\zeta v \in K^{\times p}$.

[Coh] H. Cohen, *Number Theory Volume 1: Tools and Diophantine equations*, Springer, 2007.

[Gr1] G. Gras, *Class Field Theory, From Theory to Practice*, Springer, 2003.

[Gr2] G. Gras, *Analysis of the classical cyclotomic approach of Fermat's Last Theorem*, Publications Mathématiques de Besançon, 2010.

[GQ] G. Gras and R. Quême, *Vandiver papers on cyclotomy revisited and Fermat's Last Theorem*, Publications Mathématiques de Besançon, 2012/2, 47-111.

[Qu2] R. Quême, *On Furtwängler's theorems and second case of Fermat's Last Theorem*, arXiv.org, arXiv.1304.6179.pdf

[Rib1] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[Va1] H.S. Vandiver, *Summary of results and proofs concerning Fermat's Last Theorem*, proceedings of National Academy of Sciences, Jan 6, 1926, p. 106.

[Va2] H.S. Vandiver, *Summary of results and proofs concerning Fermat's Last Theorem (second note)*, proceedings of National Academy of Sciences, Oct 21, 1926, p. 767.

[Was] L.C. Washington, *Introduction to cyclotomic fields, second edition*, Springer, 1997.